# QUANTUM COMPUTING AND QUANTUM CRYPTOGRAPHY

*Hayk Sargsyan*

*Gate42 Quantum Computing Lab*

# GATE42

- gate42.org/
- github.com/gate42qc/
- QC Armenia – facebook

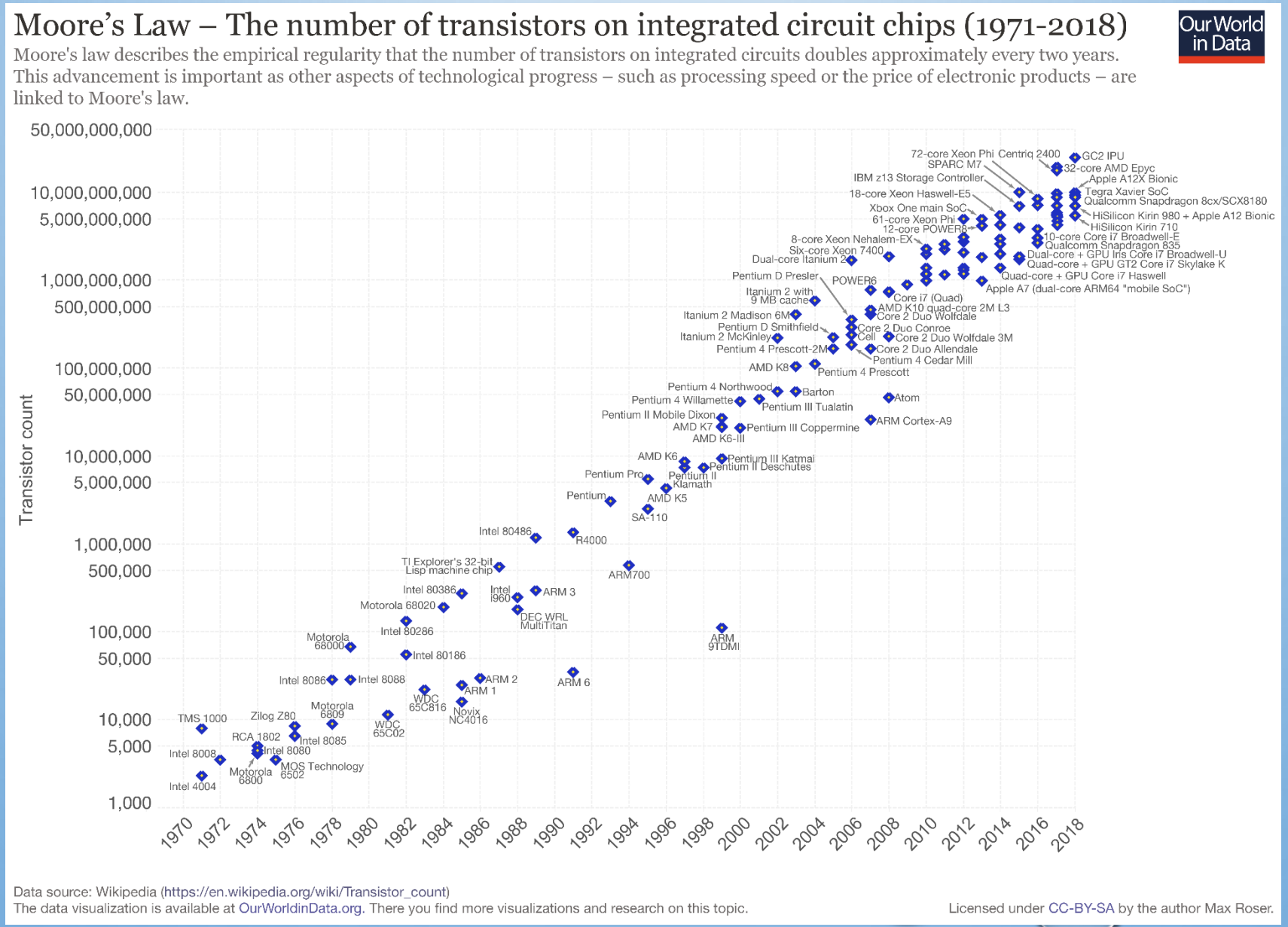
- Quantum algorithms
- Theory of QC
- Education of QC
- Popularization of QC

# «Գեղ կանգնի, գերան կկոտրի»

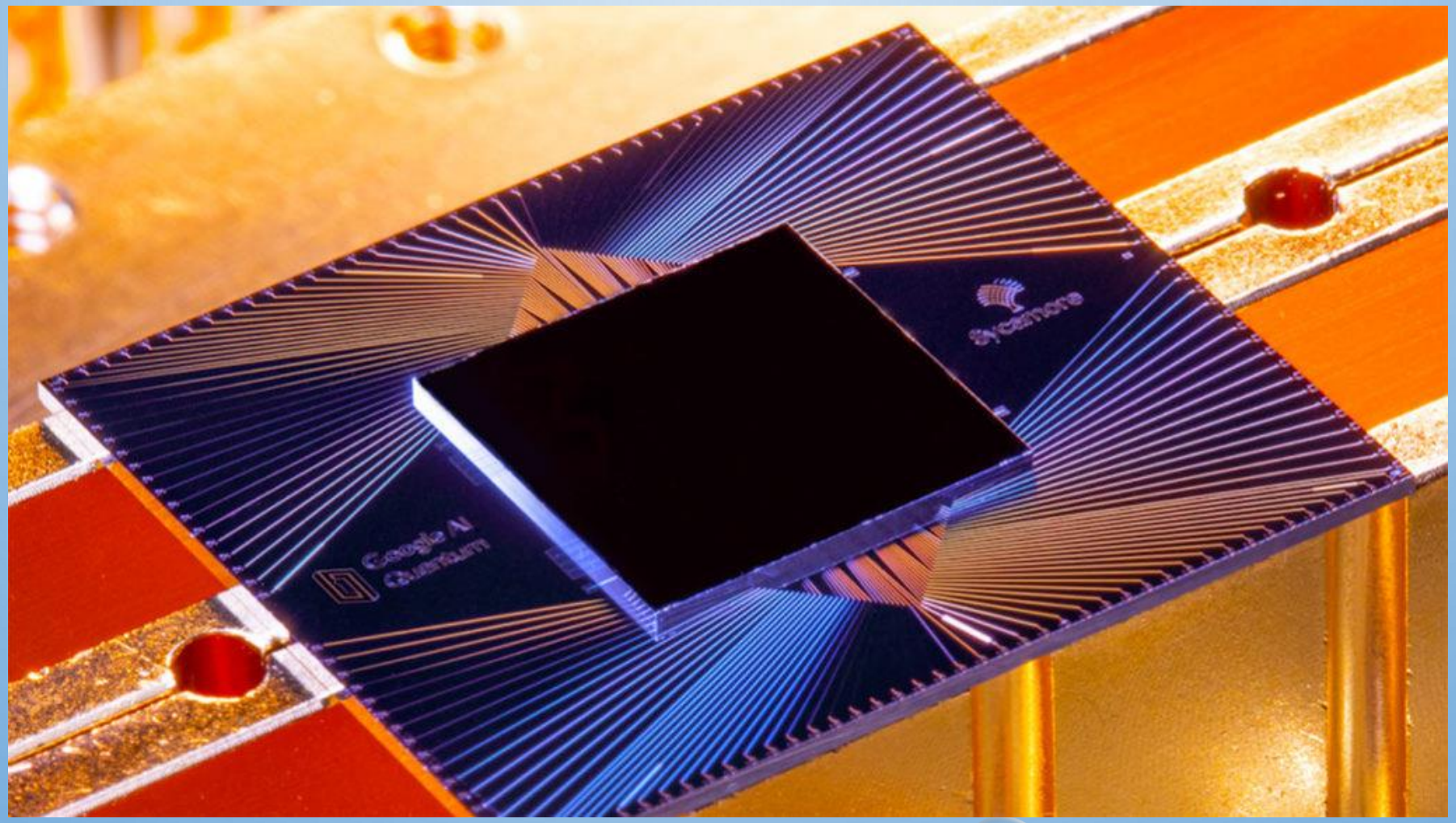
# OUTLINE

1. INTRO TO QUANTUM COMPUTING
    - *Misconceptions*
    - *Common Facts*
2. CRYPTOGRAPHY AND QUANTUM COMPUTING
    - *Classical Cryptography*
    - *RSA*
    - *Shor's Algorithm*
3. (POST)-QUANTUM CRYPTOGRAPHY
    - *Quantum Key Distribution*

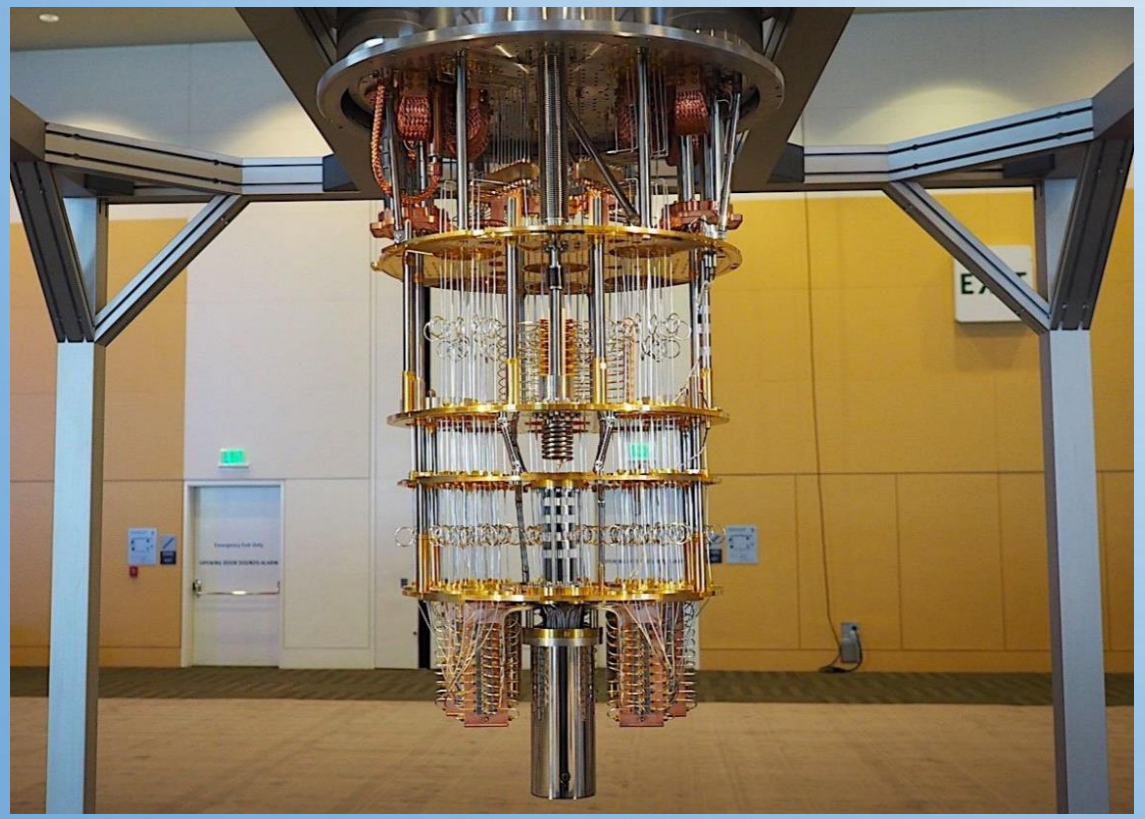
# MOORE'S STATISTICAL LAW



# GOOGLE'S SYCAMORE CHIP



# SPEED OF ELEMENTARY OPERATIONS



vs.

# SUPERPOSITION

- CLASSICAL BIT

  Only stationary states: $|0\rangle$ or $|1\rangle$

- QUANTUM BIT (QUBIT)

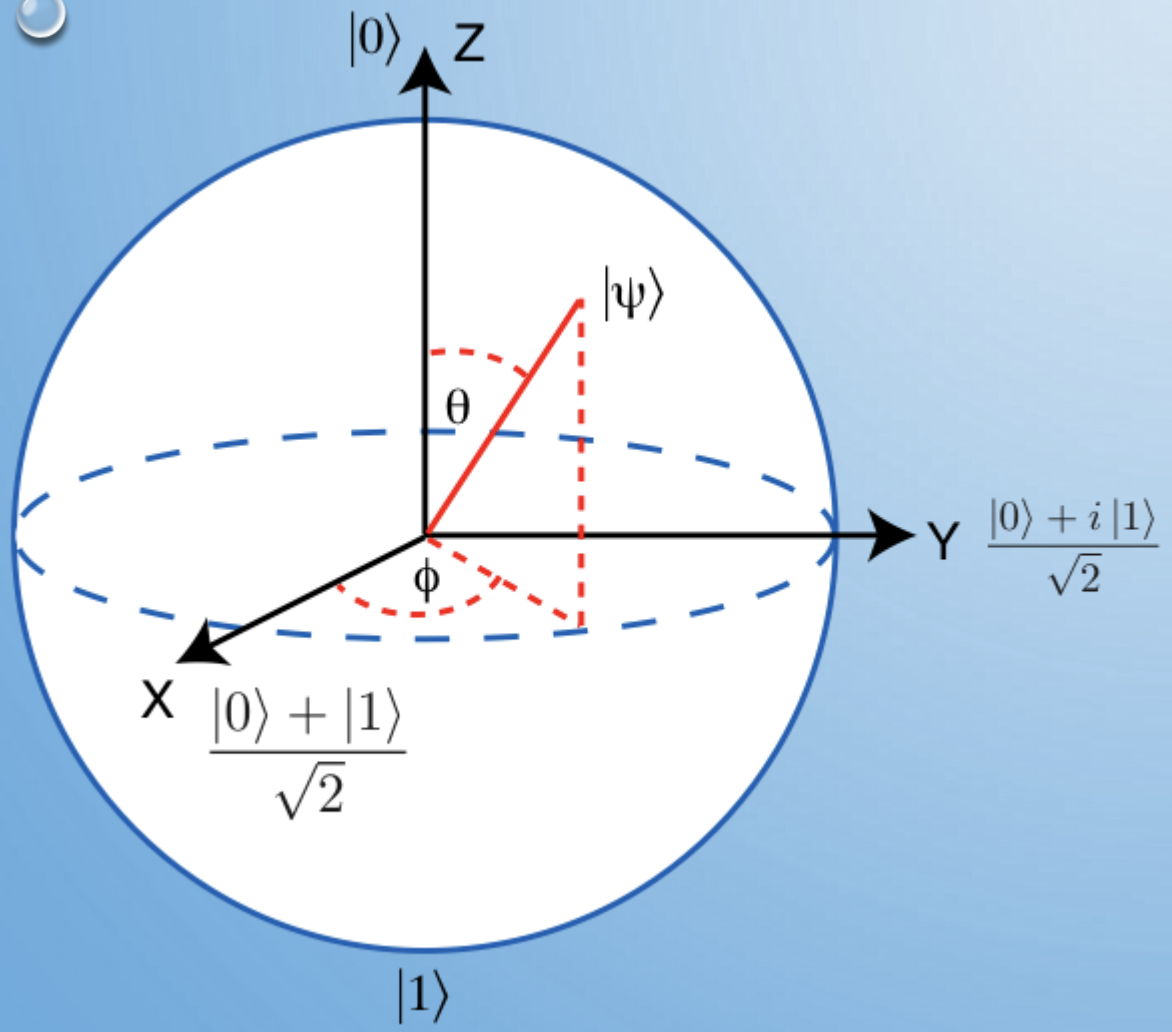
  General states (stationary and non-stationary): $\alpha|0\rangle+\beta|1\rangle$

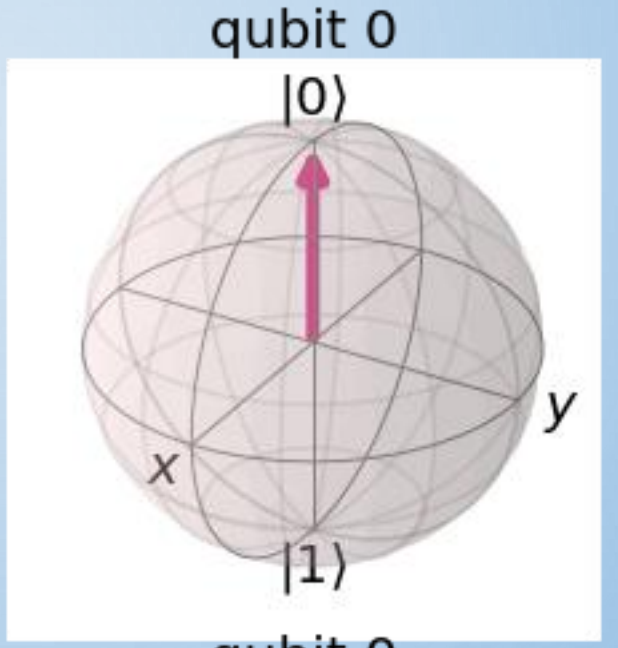
  Coefficients $\alpha$ and $\beta$ are complex numbers

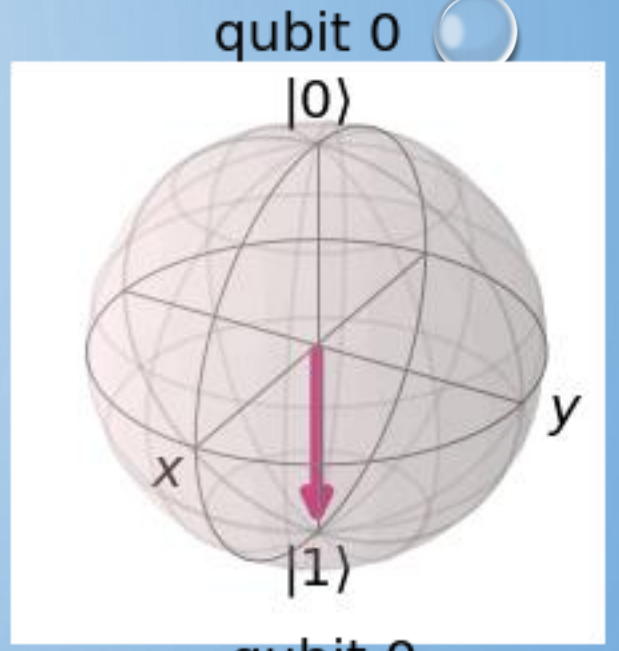
  $|\alpha|^2+|\beta|^2=1$ and global phase does not matter, so

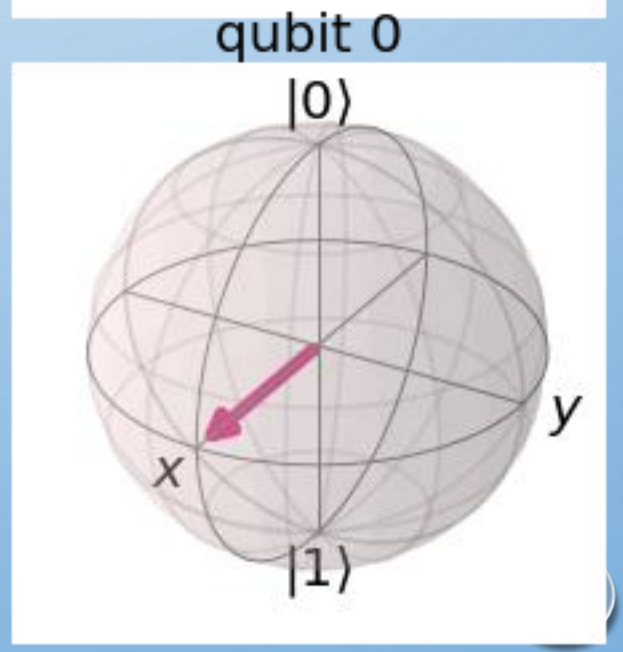
$$\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

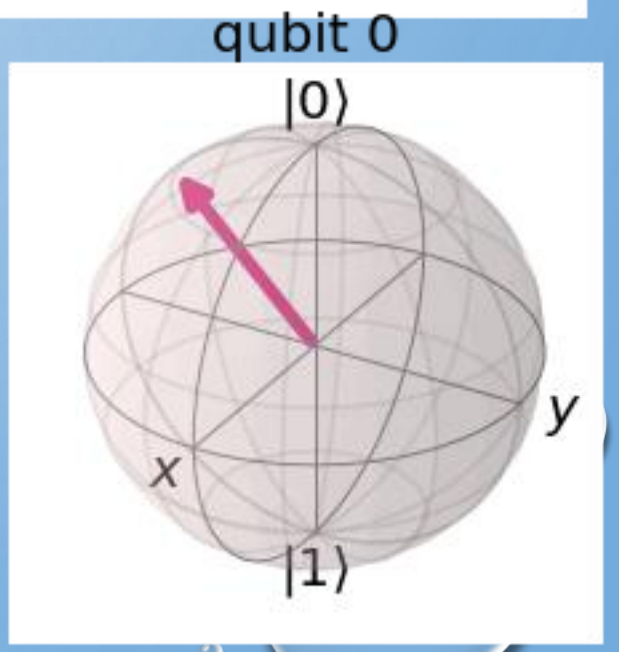
# BLOCH SPHERE



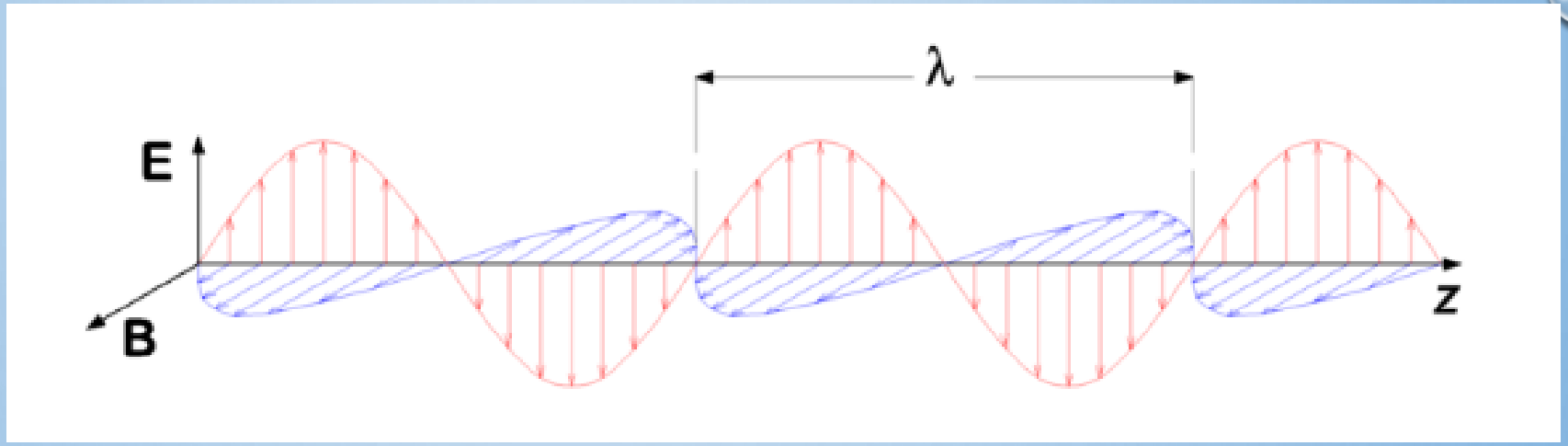



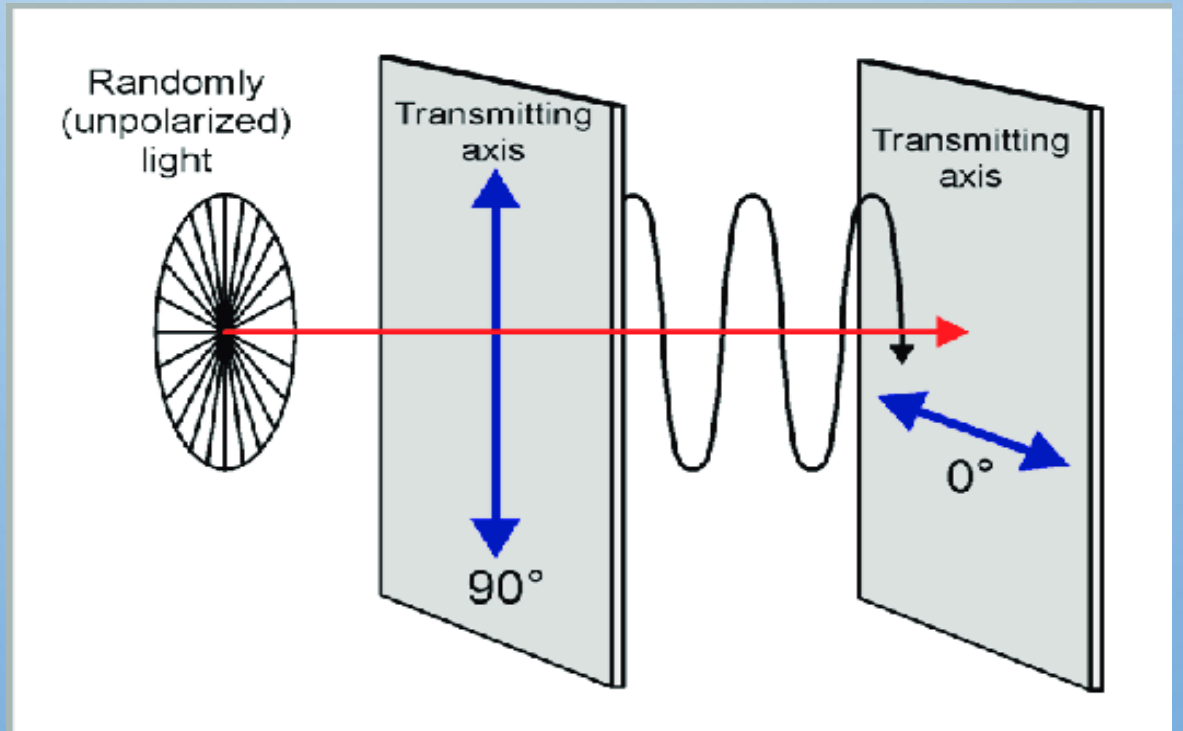



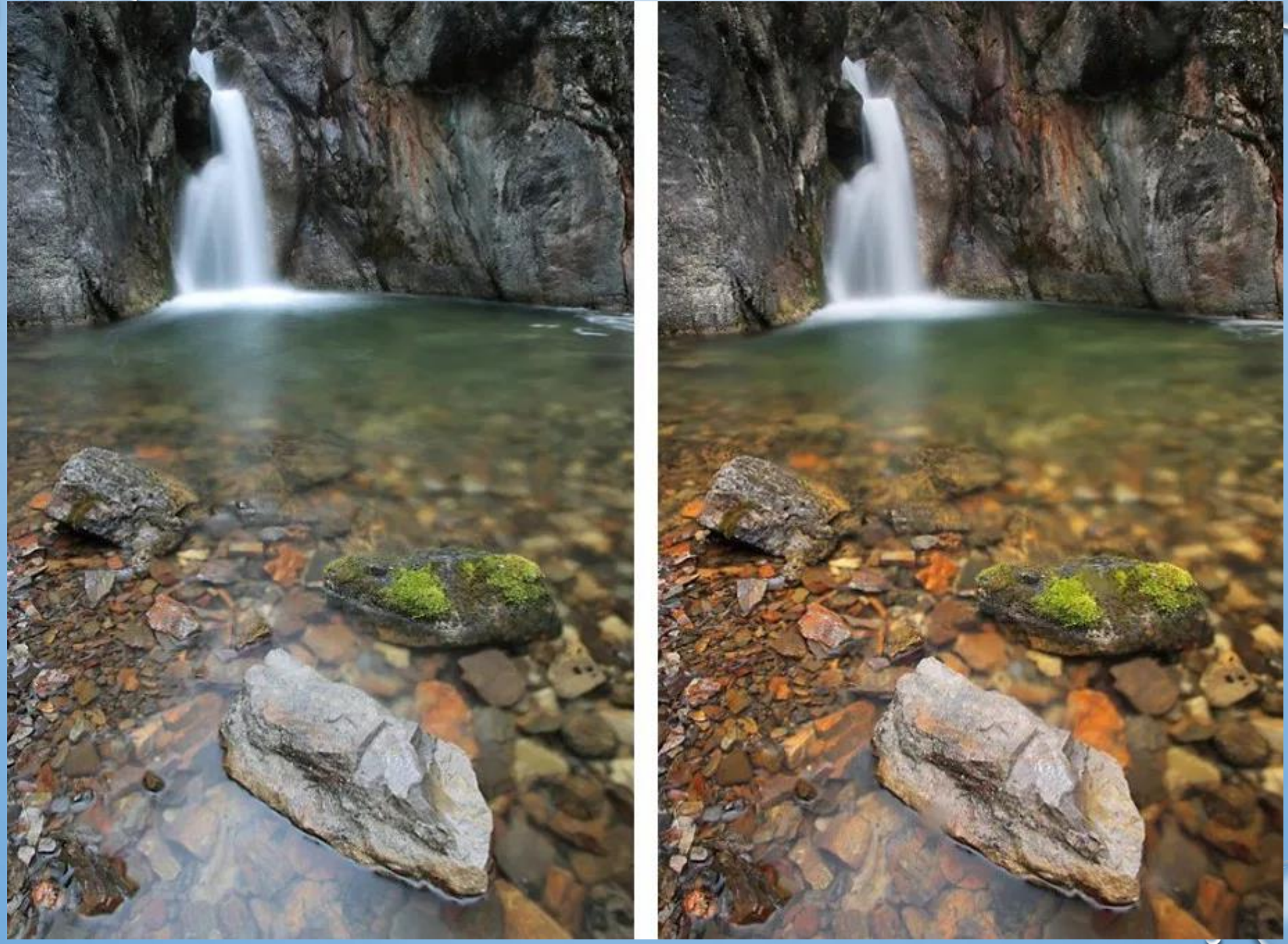
# PHOTONS AS QUBITS

- Polarization:




- Polarizing filters:





# ENTANGLEMENT

- Stationary states of n classic bits

$$|00...0\rangle, |00...1|, \ldots, |11...1\rangle$$

- n-qubit general states

$$|\psi\rangle = \alpha_0 |00...0\rangle + \alpha_1 |00...1| + \ldots + \alpha_{2^n-1} |11...1\rangle$$

- Entanglement

$$|\Phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

# QC PARALLELISM

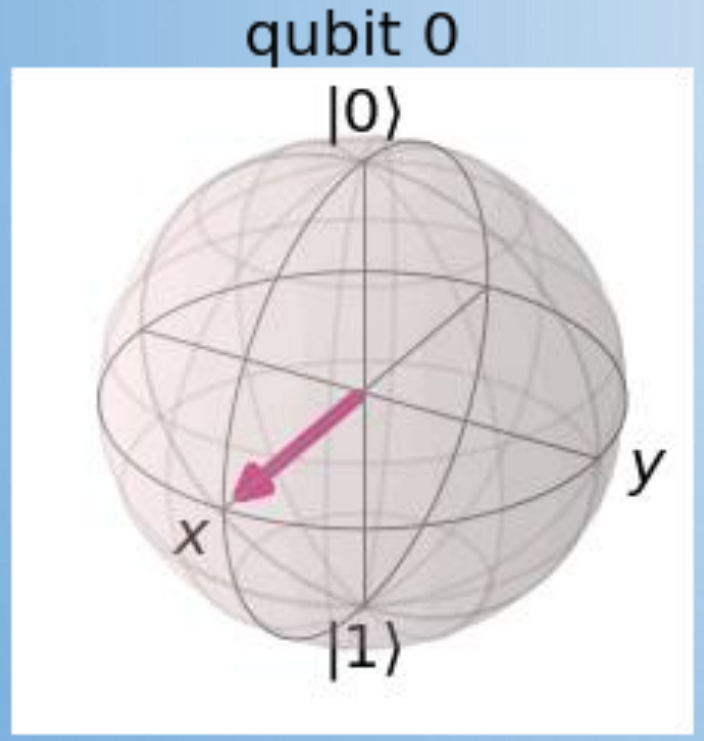
- IS QUANTUM COMPUTATION INHERENTLY PARALLEL?

  YES and NO

- QUANTUM MEASUREMENT

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \begin{cases} |0\rangle & \text{with probability } |\alpha|^2 \\ |1\rangle & \text{with probability } |\beta|^2 \end{cases}$$

# QUANTUM MEASUREMENT

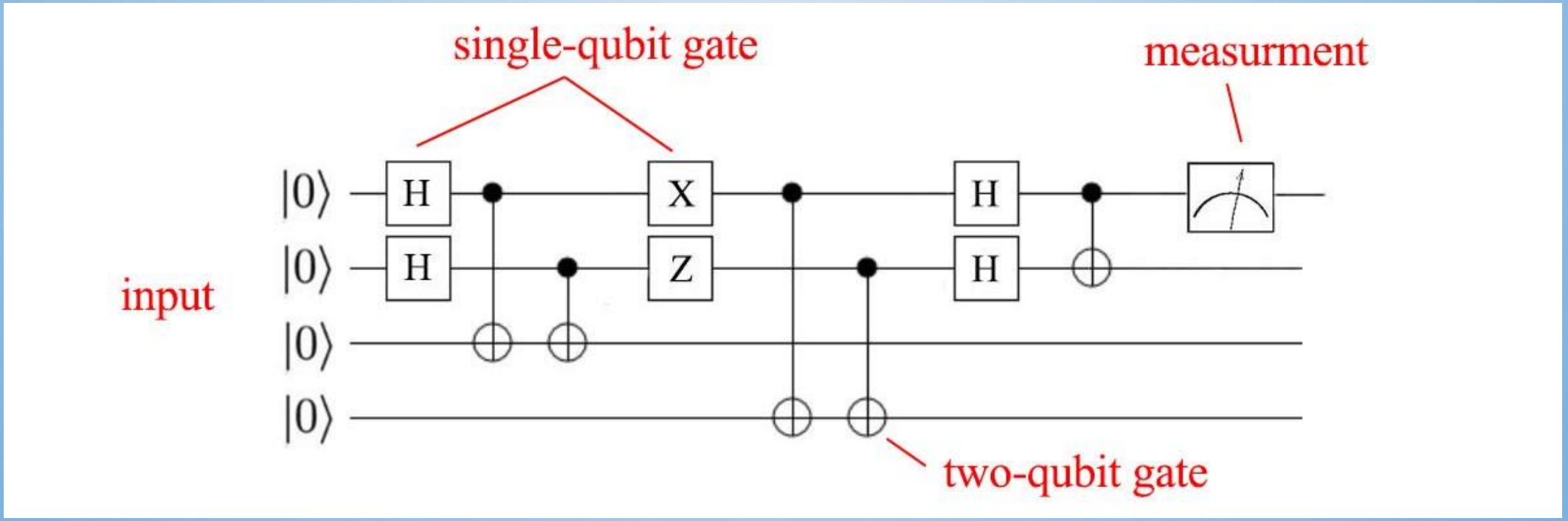



Hadamard gate

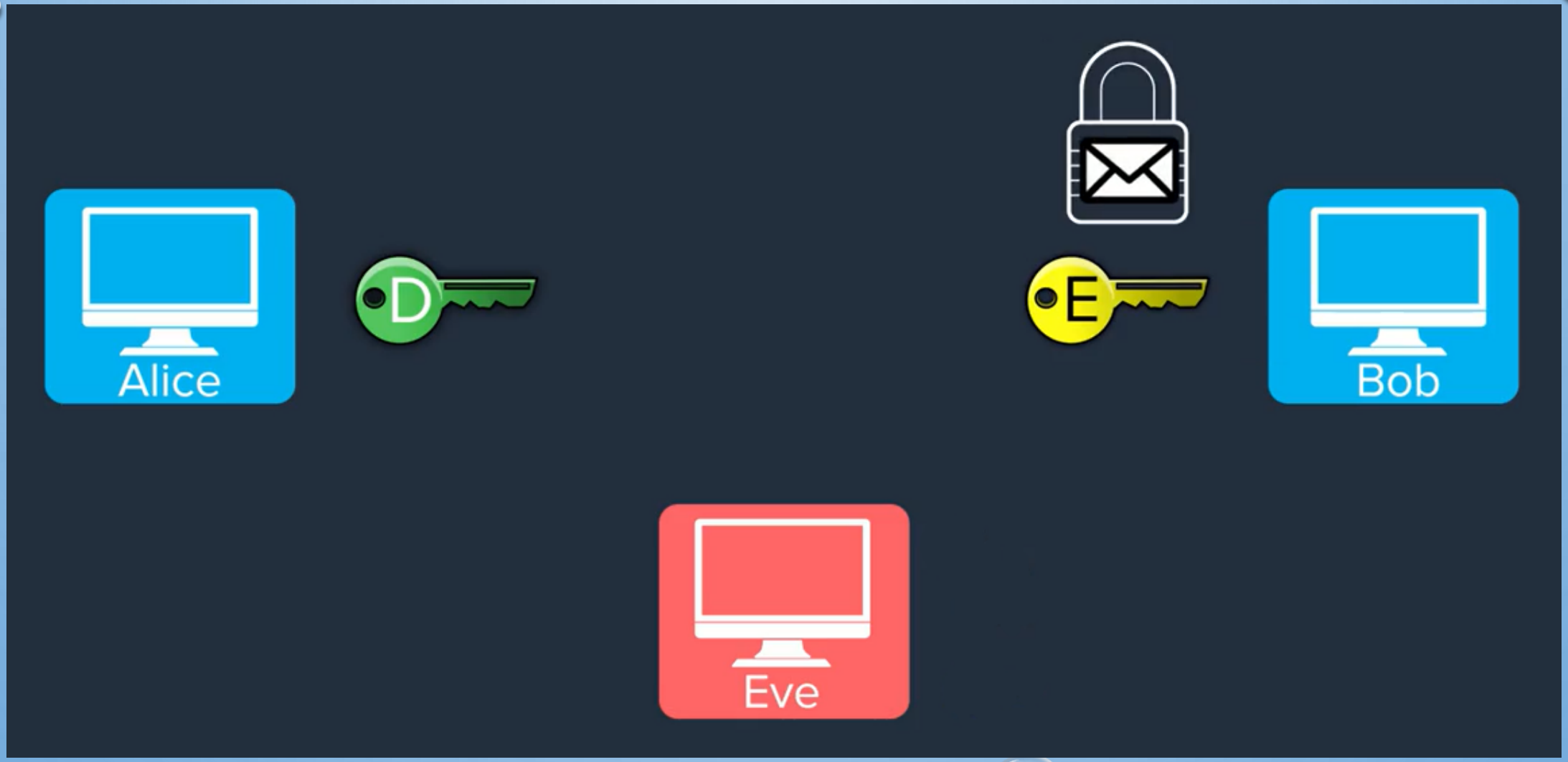
$$H|0\rangle = |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

# QUANTUM COMPUTATION

- INIT -> CALCULATE/MANIPULATE -> MEASURE

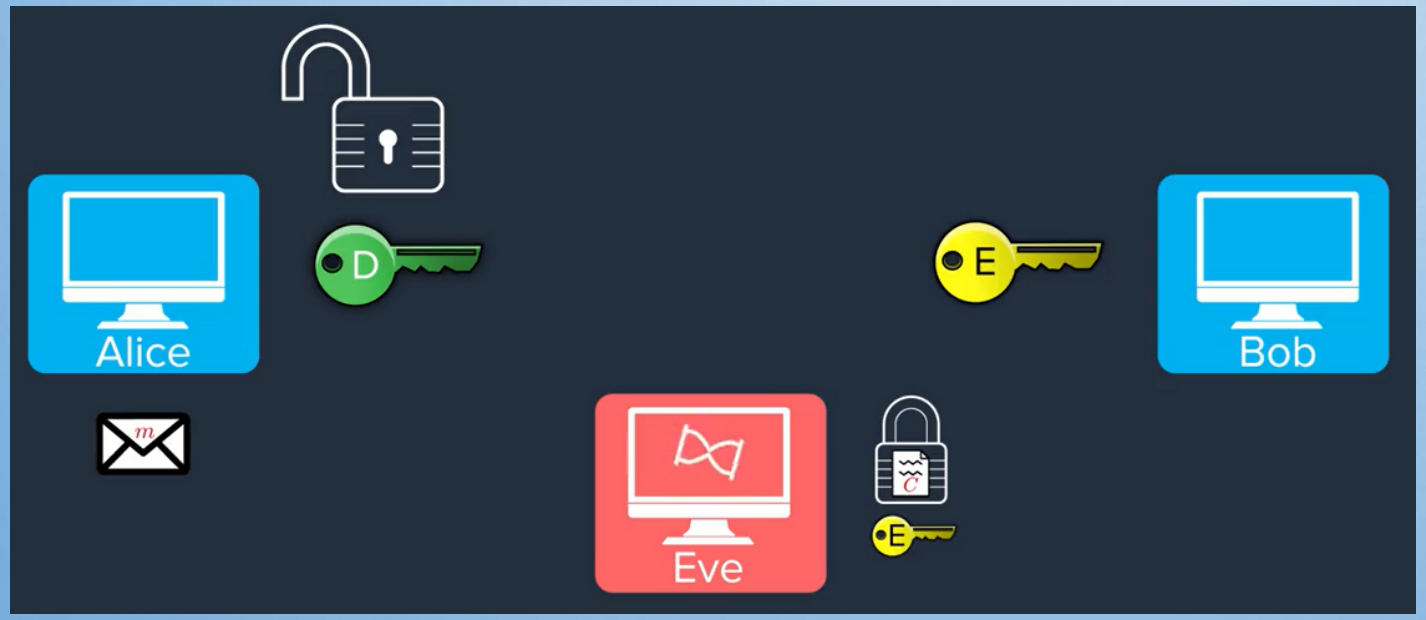


# CRYPTOGRAPHY



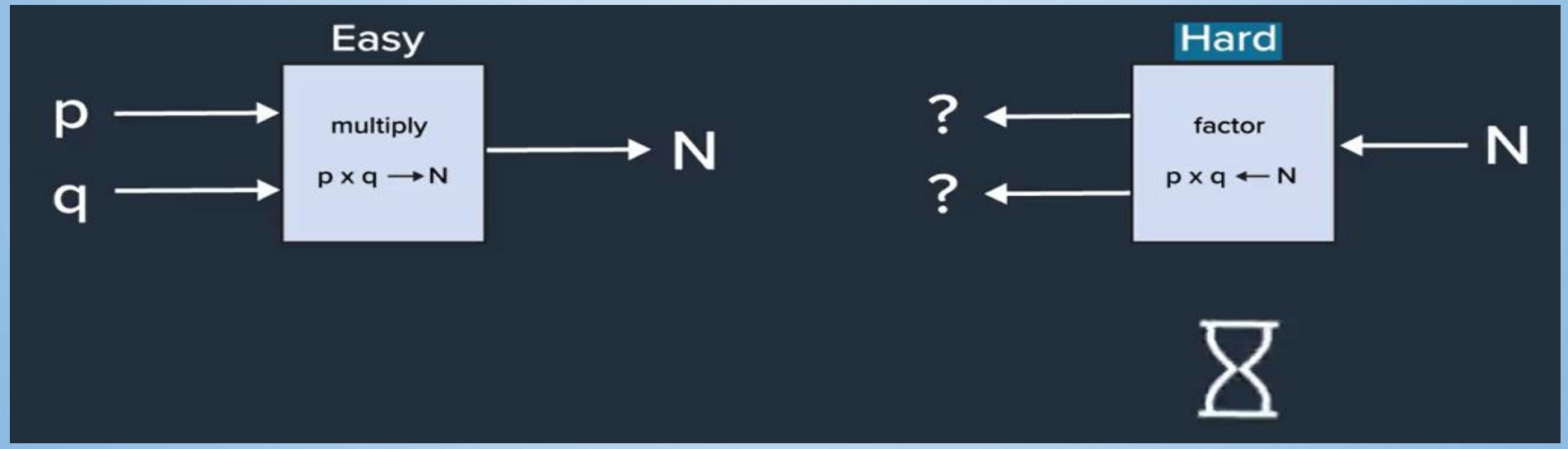
# CLASSICAL CRYPTOGRAPHY

- Symmetric key cryptography
- Asymmetric (public) key cryptography




One way functions:

# RSA




The basic idea behind RSA (modular exponentiation): $\left(m^e\right)^d = m \pmod{N}$

m: numerical representation of Bob's message

e: the key for encryption

d: the key for decryption

N: a laaarge integer (part of both encryption and decryption)

# RSA IN STEPS

- KEY GENERATION AND DISTRIBUTION
  - Bob wants to send a message to Alice
  - Bob asks Alice to send the public keys N and e
  - Alice keeps the decryption key d private
- ENCRYPTION
  - Bob converts his message into a numerical representation m
  - Bob calculates $c = m^e \pmod{N}$
  - Bob sends c to Alice
- DECRYPTION
  - Alice receives c
  - Alice calculates $c^d \pmod{N} = m$
  - Alice reconstructs Bob's message from m

# KEY GENERATION IN DETAIL

- Generate 2 random prime numbers p and q
- Generate the number $N = pq$
- For any number $x < N$

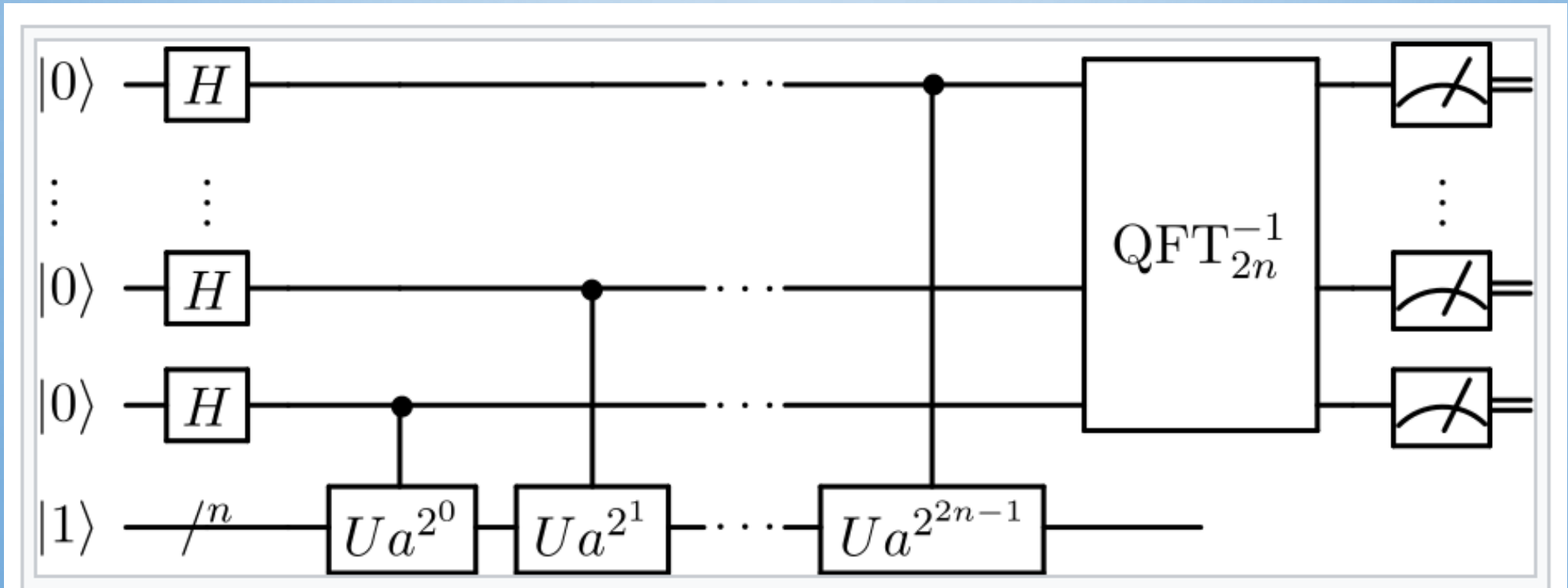
  The period r of modular exponentiation $f(x) = a^x \pmod{N}$

  is related to p and q $\frac{(p-1)(q-1)}{r} = \text{even integer}$
- Public and private keys e and d respectively

$$1 \prec e \prec r \qquad ed = 1 \pmod{r}$$

# SHOR'S ALGORITHM

- A quantum algorithm for period finding
- Exponentially faster than the best classical algorithm



# EXPERIMENTAL REALIZATIONS

- 2001 – Factor 15=5*3
- 2012 – Find once again 15=5*3
- 2012 – Factor 21=7*3

# QUANTUM SUPREMACY

- 2019 – Google announces about quantum supremacy
- What does quantum supremacy mean?

# IS QUANTUM EVIL?

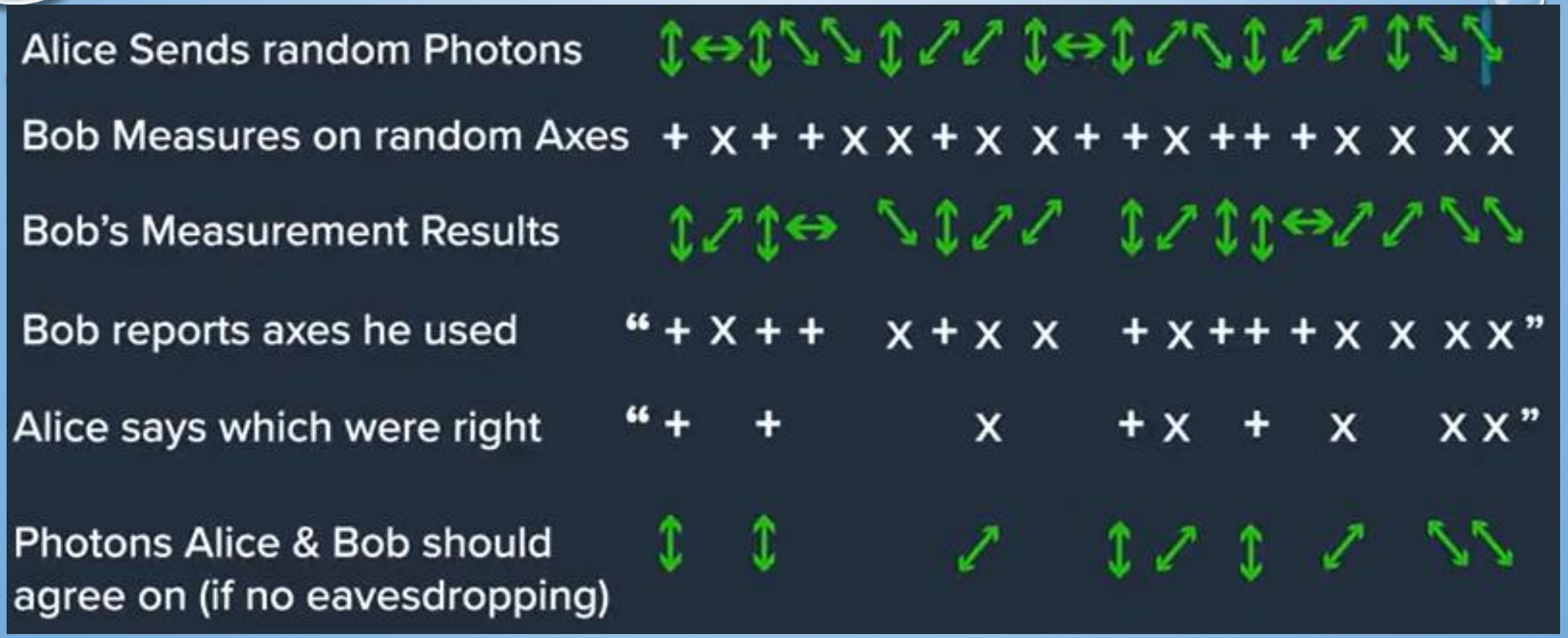
# QUANTUM CRYPTOGRAPHY

- QUANTUM COMMUNICATION CHANNELS
- QUANTUM KEY DISTRIBUTION (QKD)
- QUANTUM CRYPTOGRAPHY

# NO-CLONING THEOREM

- NO PROCESS CAN COPY A GENERAL QUANTUM STATE $\alpha\,|0\rangle + \beta\,|1\rangle$

# QKD: BB84




Other protocols: BBM92, E91

# THANK YOU!